Testimony by:
Rodney Cain, Chief Information Officer and Vice President
HealthBridge

HIT Standards Committee
Hearing on Health Information Technology Security Issues, Challenges, Threats, and Solutions

For the Data Theft, Loss, and Misuse Panel:

Thank you for the opportunity to speak today on such an important topic. As the Chief Information Officer for one of the nation's largest health information exchanges, I feel I have the professional duty to reflect on this topic at some length. This topic is one that as a CIO keeps you up at night — are we keeping our community's data secure? Our hospitals, our physicians, and ultimately the patients in our community are trusting us to keep their data safe. Are we doing our job to keep the bad guys out?

As we continue to grow and expand our services across our community, it becomes increasingly important that we constantly evaluate our processes, and be ever more vigilant even than when we created the exchange 13 years ago. Today, I would like to offer some of our real-world experience operating a diverse community-based network and how we balance usability with the need to defend our data against rare but untenable events of theft, loss or misuse.

To help set the stage, let me give you some background on my organization. Founded as a not-for-profit corporation in 1997, HealthBridge has grown to one of the nation's largest and most successful community-based health information exchange organizations. Our original goal was to enhance our ability to share clinical information electronically in the Greater Cincinnati, tri-state area. Today, HealthBridge connects 24 hospitals, more than 700 physician practices, 17 local health departments and dozens of other health care entities including commercial labs, diagnostic centers, and nursing homes, among others. In a metropolitan area of 2.1 million people, we have 2.8 million patients in our master patient index and we have been able to achieve a very high adoption rate in our community, with roughly 90 percent of physicians in our service area participating.

Each month more than 3 million clinical lab tests, radiology reports, orders, and other clinical information are transmitted through our network. At HealthBridge, we have made it a core part of our operations to ensure that this large amount of clinical data remains confidential and secure while also facilitating timely and accurate availability of this information for the clinicians treating patients.

From our experience, the setting in which the desire for ease of use and the need for security are most delicate is the physician practice itself. Practices are already busy and

we have seen first hand that a complicated or cumbersome process to access systems will hurt adoption rates. Depending on their size, practices also tend to be less sophisticated than larger organizations with regard to security and IT in general. And to further complicate matters, most of our physicians just don't want another password to remember, they want to treat their patients. This situation presents a difficult challenge, and we have to work hard to strike a balance between usability and security.

To this end, we have developed a variety of strategies to prevent theft, loss or misuse but still allow easy access to our systems. One tool is the full use of role-based access controls, which allow us to impose greater controls, and a greater burden on those users that have the most privileged access. So, users with access to clinical information have more steps to authenticate, are prompted more often with security challenge questions, and are logged off sooner than those with administrative access only. By not employing a one size fits all solution across our community, we can raise awareness about security, provide protection of our data, and not create so many barriers that our systems ultimately are not used. This would seem almost obvious, but in our experience many of the software applications we work with do not have the flexibility to support a health information exchange, which supports multiple separate health organizations, not a single enterprise.

Another tool, or really a partner in managing security, is the practice administrator. We engage our practice administrators with a variety of management tools and processes to assist them in maintaining the security and access to their data. For example, they are forced to review and acknowledge users and roles on a recurring basis. Any changes are logged, audited and approved by the HIE.

We also maintain a community directory of health care workers, so our system can recognize when an account for a user is requested in a new location or with a new organization. We can then verify if that user is authorized to access information in both locations and act appropriately. Because health care workers change jobs so frequently, we proactively disable user accounts if they are not used for a set period of time, again based on role.

These and many other security practices have been developed in coordination with our hospital and physician community in over a decade of operations. But in the rapidly evolving environment we have today, other HIEs do not have that luxury of years to develop their own strategies and best practices to prevent theft, loss and misuse.

This is one reason that HealthBridge in recent years has established a network of health information exchange organizations called Collaborating Communities which has allowed us to assist with the rapid establishment of new operational health information exchanges. Under this model, HealthBridge shares its technology infrastructure and best practices with other community exchanges. This model gives the new exchange the

ability from day one to have a robust infrastructure for protecting clinical information without huge capital outlays upfront.

We have found that having a template that an exchange can readily use ensures they have what is needed up front and both facilitates rapid implementation and a high level of best practice adoption. From day one the exchange is able to share data in a highly secure manner because they have both technology and business practices in place to verify who is sending information, to ensure the clinical information is transported securely, and to know a user is authorized to see it.

In this way, we have observed that standards can be very powerful. The work this committee is doing to develop those standards and best practices and to communicate them to the nation is absolutely critical. It helps ensure that health care providers, health information exchanges, communities and states are better prepared for the new world of secure, electronic information sharing.

HealthBridge currently serves as an agent for sharing information among providers. As we look ahead, one of the challenges we see is how to best ensure that clinical data is also available to patients. It is one thing to manage 800,000 logins a year from providers that our staff physically visits and interacts with regularly. It is quite another to give access to potentially millions of health care consumers, while protecting against data theft, loss or misuse. Standards for minimum levels of user identity verification, authentication, and authorization on the use of data will be vitally important as we move forward.

Thank you again for this opportunity to share my experiences and work in health information exchange and with protecting clinical information. I am happy to answer any questions from the committee.